Draft DoD Position

Regarding X.25

1. Introduction

The International Telecommunications Union (ITU) through its International Consultative Committee on Telegraphy and Telephony (CCITT) has been developing a recommendation for the interfacing of subscriber computers to public Packet Switched data networks. This recommendation is designated X.25 and specifies the procedures and formats by which subscriber data termination equipment (DTE) can exchange packets the public data network data circuit termination equipment (DCE).

Recommendation X.25 also makes reference to lower level-line control procedures and electrical interfacing options compatible with the so-called X.25 "packet level" interface protocol. The lower level data link control procedures include the CCITT/ISO High Level Data Link Control procedure (HDLC) and a version of the IBM Bisynchronous Link Control procedure ("Bisync"). The electrical interface recommendations include CCITT recommendations X.21, V.24 and V.35.

These recommendations, taken together, constitute the body of the X.25 electrical, link and packet layer protocols which form the lowest three levels of the International Standards Organization's Open Systems Architecture model.

In addition to the X.25 recommendation, CCITT has also proposed other recommendations for interconnecting public data networks (X.75) and for interfacing computer terminals to public data networks (X.28, X.29).

The principal mode of operation of the X.25 interface is "virtual circuit" oriented. The subscriber DTE initiates a virtual circuit set-up procedure within the public data net by sending to the public data net a connection request packet. Once the virtual circuit is established, the public data net returns a connection accept packet and the source and destination DTE's can then exchange data packets.

A receiving DTE, upon receiving a connection request packet can accept or reject it. If the connection is rejected, the source DTE is informed of this by the public data net.

The X.25 interface procedures include support for flow control between networks could not be used effectively, if at all, if the only interface to them had to adhere to the X.25 recommendations.

Examples of broadcast or semi-broadcast, DoD packet networks include packet satellite, packet radio, Ethernet, Mitrebus, PLRS (position location reporting system) and JTIDS (joint tactical information distribution system). What is common about these nets is the fact that access to the common communication resource is shared in time, often by means of contention detection and resolution methods. This method of sharing access to a common communication capacity (e.g. radio channel, satellite transponder, coaxial cable) is extremely efficient for large numbers of bursty traffic sources, particularly mobile ones. By comparison, circuit-like sharing of these resources would be very wasteful of the capacity.

More to the point, however, is the fact that sequencing and integrity are services which are not desirable to build into such multi-access nets. In order to sequence and maintain the integrity of the packets emitted by a source DTE, the subnet must be prepared to retransmit packets internally and to buffer them at least at the destination DCE to assure re-ordering, if necessary, before delivery to the destination DTE.

In mobile networks, or in systems where local jamming or other hostile action is likely, such services merely introduce congestion if packets which have arrived at the destination cannot be delivered because the "next" one hasn't arrived yet and also introduce large variation in packet inter-arrival time at the destination DTE. The attempt to maintain integrity may also congest the net other than at the destination if the destination is out of contact (e.g. jammed, destroyed, beyond line-of-site, etc.) but this fact isn't yet known to the rest of the network.

The consequences of sequencing within a network are grave if the net is intended for real-time data services such as fire control, tracking and so on. Furthermore, it has been found that the delay variations introduced by attempting to maintain sequencing and integrity within such nets makes it impossible to support integrated packet voice services as part of the data net. Insisting on only X.25 virtual circuit services would render wasted an enormous DoD investment in securable, low data-rate packet speech technology.

Moreover, the point-to-point nature of X.25 renders useless the broadcast (multipoint) nature of nets such as Ethernet or the DARPA

Atlantic Packet Satellite Net (SATNET). These systems allow a single transmission to be received by multiple receivers. This is also a feature common to JTIDS, PLRS and a multitude of U.S. Navy command/control communication systems. If integrity and sequencing were part of the subnet service, the source DCE would have to retransmit packets until it had gotten acknowledgements from all destination DCEs (or even DTEs). But in hostile conditions, not all DTEs or DCEs will be accessible.

Apart from its potentially disastrous imposition of sequencing on multi-point communication services, recommendation X.25 also does not deal explicitly with communication security and precedence, both of which are important to the U.S. Department of Defense.

As a consequence of many of these considerations, the majority of the experimental U.S. Defense packet networks have been organized around the concept of datagrams. A datagram is a finite string of bits containing a header which typically indicates the destination address to which the bitstring is to be sent, often indicating the source and other relevant information such as length, type of transmission service desired, precedence and so on. Datagrams typically are transported independently of each other by the packet networks, imposing few network mechanisms to implement or use the simple and not necessarily reliable or sequential datagram service.

The Department of Defense would not be well-served, if all its packet communication systems had to provide service through interfaces meeting recommendation X.25 provisions.

By the same token, however, neither would the Department of Defense be well-served if it could not make use of the restricted services provided by nets offering only X.25 interfaces.

During its exploration and development of packet switching techniques, the Department of Defense has pursued the development and test of a layered protocol architecture which permits a broad range of different packet networks types to be interconnected and used end-to-end, despite the very significant variations in the classes of services they offered, their different interfaces, speed of operation, throughput and maximum packet sizes.

At the heart of this layered architecture is an Internet Protocol (IP) which relies only on the most primitive datagram service from each constituent network of the Internet System. Figure 2 illustrates the relationships among the protocol layers of the DoD Internet Architecture.

The important differences between the DoD Internet Architecture and the networking models developed by CCITT and ISO are:

D1. The specific existence of an internet layer.

D2. The concept of gateways external to the communication subnet.

D3. The use of encapsulation to transport internet packets through intermediate networks.

D4. The concept of gateway fragmentation and host (DTE) reassembly.

D5. The assumption that the basic network service is datagram and not virtual circuit.

D6. The provision for many network interfaces including X.25.

D7. The explicit provision for security and precedence in the internet protocol.

D8. The coalescing of the OSI Session and Transport layers into a single transport layer and the re-naming of the presentation layer to be the utility layer.

The encapsulation concept, along with the explicit provision of an internet protocol layer based on datagram services has made it possible to implement, exercise and use daily the protocol hierarchy illustrated in Fig 3.

While only the Internet Protocol, Internet Control Message Protocol and Transmission Control Protocol are ratified DoD standards, the other protocols are in widespread use in the experimental DoD Internet System which includes public networks (U.S. Telenet, UK PSS and IPSS) as well as experimental defense networks in the UK (Royal Signals and Radar Pilot Packet Switched Network) and Norway (Norwegian Defense Research Establishment--NDRENET).

Creation of the separate gateway system has made it possible to incorporate into the DoD Architecture mechanisms for recovering from partitioning of a communication subnet by routing traffic through the internet gateway system as illustrated in Fig. 4.

The encapsulation and fragmentation mechanisms at the internet level have allowed internet routing to be decoupled from the problem of accommodating varying maximum packet sizes in each network. The strategy allows the network packet size to be optimized to the particular switching and transmission technology (as well as local communication and propagation conditions) in each network (Fig. 5).

By assuming only datagram services from each constituent network, the DoD Internet Architecture is able to support a broader range of applications including real-time packet voice. Each internet packet can include an indication of the type of service it needs, which might trigger the use of virtual circuits on some networks which provide the service, but in general, virtual circuit-like service is provided by the Transmission Control Protocol at the transport layer, outside the collection of interconnected packet subnets.

The simplifying datagram service assumption also makes it easier to use multiple gateways to share traffic loads since it isn't necessary to maintain sequencing and integrity of any particular virtual circuit passing across a given network. Packets can be switched to alternate gateways as appropriate to share their capacity. This also helps to speed up recovery when gateways fail without necessarily requiring action on the part of the source DTE (host).

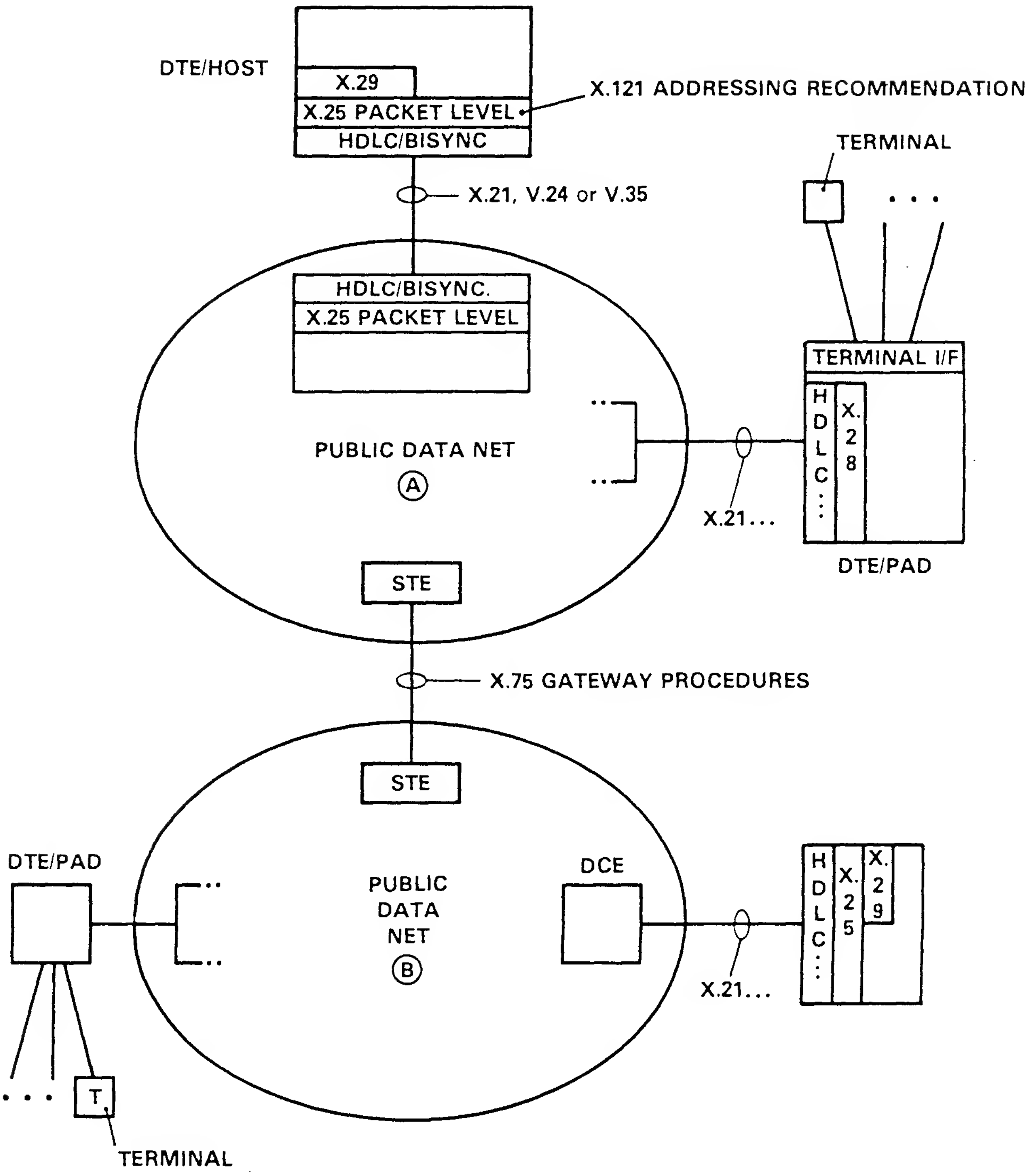
The details of the security architecture for the DoD Internet System are classified, but it can be mentioned that provision for both link-by-link and end-to-end security has been made, as well as accommodation for multi-level security protection.

The U.S. Defense Advanced Research Projects Agency (DARPA) is currently conducting experiments with its counterparts in Norway (Norwegian Defense Research Establishment), the United Kingdom (Royal Signals and Radar Establishment), and Germany (DFVLR--the German Air and Space Research Agency) on the use and further development of the Internet Architecture. These experiments are relevant to the on-going discussion among NATO countries concerning NATO standards for packet communication, and their results should be factored into any decisions and agreements reached within the NATO normalization and standardization process.

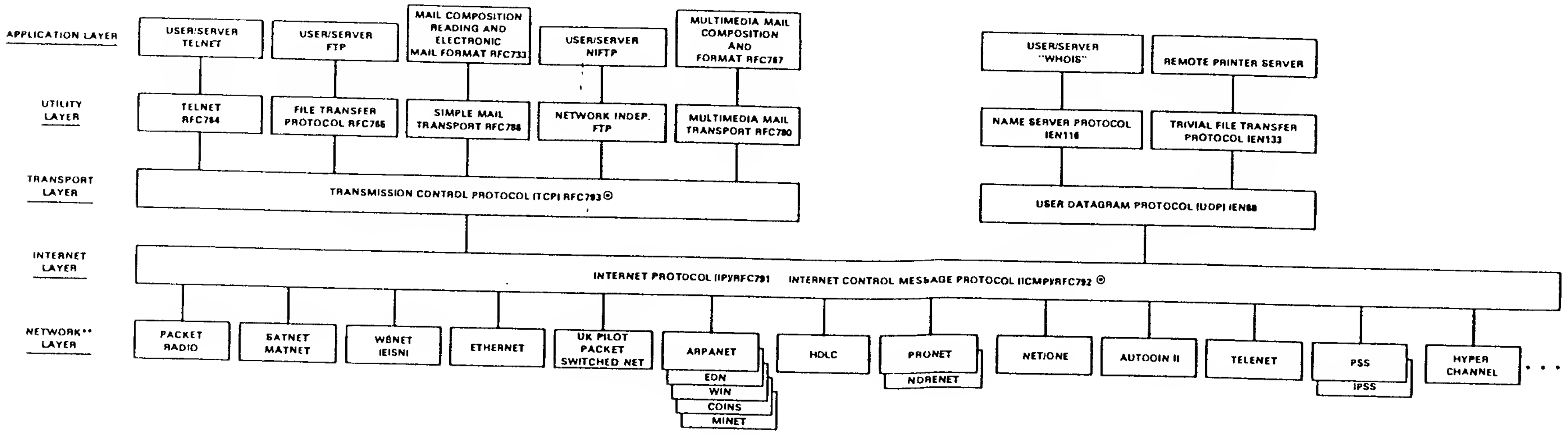
2. The U.S. Department of Defense Position on Recommendation X.25

In view of the foregoing, it is the U.S. Department of Defense position that an acceptable U.S. or NATO standard network architecture must be able to make use of, but not be limited to, networks providing interfaces meeting the CCITT Recommendation X.25. In particular, provision for non-virtual circuit modes of operation are considered mandatory to support transaction or real-time applications in an internetwork environment.

FIGURE 1 ILLUSTRATES THE APPROXIMATE
RELATIONSHIPS AMONG THE VARIOUS RECOMMENDATIONS



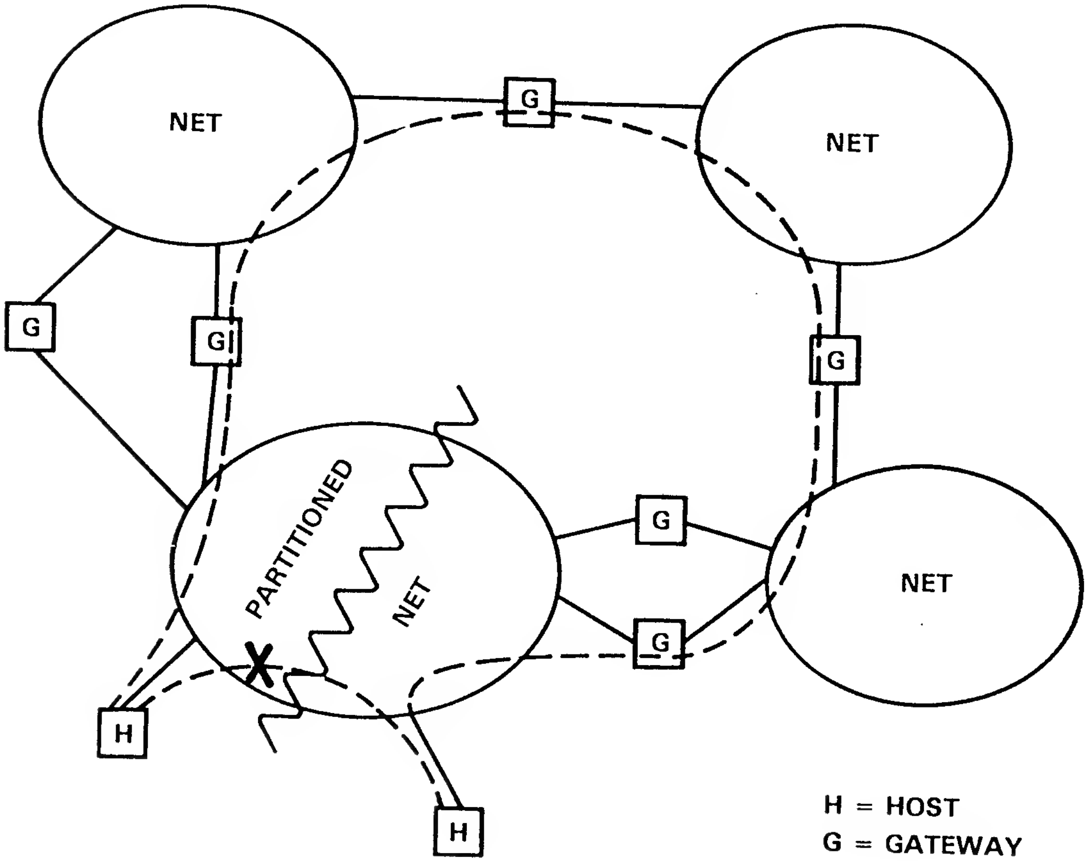
CCITT PROTOCOL RECOMMENDATIONS
FIGURE 1


APPLICATION LAYER
UTILITY LAYER
TRANSPORT LAYER
INTERNET LAYER
NETWORK** LAYER
USER/SERVER TELNET
USER/SERVER FTP
MAIL COMPOSITION READING AND ELECTRONIC MAIL FORMAT RFC733
USER/SERVER NIFTP
MULTIMEDIA MAIL COMPOSITION AND FORMAT RFC767
USER/SERVER "WHOIS"
REMOTE PRINTER SERVER
TELNET RFC764
FILE TRANSFER PROTOCOL RFC765
SIMPLE MAIL TRANSPORT RFC788
NETWORK INDEP. FTP
MULTIMEDIA MAIL TRANSPORT RFC780
NAME SERVER PROTOCOL IEN116
TRIVIAL FILE TRANSFER PROTOCOL IEN133
TRANSMISSION CONTROL PROTOCOL (TCP) RFC793⊙
USER DATAGRAM PROTOCOL (UDP) IEN88
INTERNET PROTOCOL (IP)/RFC791
INTERNET CONTROL MESSAGE PROTOCOL (ICMP)/RFC792 ⊙
PACKET RADIO
SATNET MATNET
WBNET (EISN)
ETHERNET
UK PILOT PACKET SWITCHED NET
ARPANET
EDN
WIN
COINS
MINET
HDLC
PRONET
NORENET
NET/ONE
AUTODIN II
TELENET
PSS
IPSS
HYPER CHANNEL
. . .

⊙VALIDATED DOD STANDARDS

** SEE APPENDIX FOR FURTHER DETAILS

DOD PROTOCOL HIERARCHY
FIGURE 3



PARTITIONED NET RECOVERY
FIGURE 4